Implementasi Pencegahan ARP Spoofing menggunakan VLAN dan Bandwidth Management

Haryogi U.S.S.K
siswantoyogi@gmail.com

Nina Hendrarini
Nina2bdg@yahoo.com

Setia Jul Ismail
Jul@politekniktelkom.ac.id

Program Studi Teknik Komputer

Politeknik Telkom Bandung

2011

ABSTRAK

Pada Proyek Akhir ini akan dibahas tentang implementasian *VLAN* dan *Bandwidth Management* dalam pencegahan *ARP Spoofing*. *ARP Spoofing* merupakan cara untuk memanipulasi pemetaan *ARP Cache*. *ARP Spoofing* akan membuat paket *ARP Reply Palsu* dan dikirimkan secara terus- menerus. *ARP Spoofing* juga biasanya diikuti dengan serangan untuk menangkap atau mengambil alih komunikasi yang tidak terenkripsi atau tidak memiliki digital signature. Kemudian dilakukan analisa terhadap simulasi program *ARP Spoofing* yang dibuat, dan diharapkan dapat memberi solusi dengan mengimplementasikan *VLAN* dan *Bandwidth Management* dalam jaringan lokal agar komunikasi yang terjadi tidak dapat disadap atau diambil oleh.

Kata kunci: VLAN (Virtual Local Area Network), Bandwidth Management, ARP (Address Resolution Protocol) Spoofing

1. PENDAHULUAN

1.1 Latar belakang

Seiring dengan kemajuan jaman, perkembangan teknologi semakin berkembang dari waktu ke waktu untuk memudahkan manusia dalam menyelesaikan pekerjaan yang akan dihadapinya. Perkembangan ini terjadi karena manusia selalu berpikir alangkah baiknya ada program(*hardware/ software*) yang dapat membantu-nya dalam menyelesaikan pekerjaan yang akan dilakukannya sehingga pekerjaan yang dilakukannya akan terasa mudah.

Salah satu dari perkembangannya adalah jaringan komputer. Jaringan komputer adalah sebuah sistem yang terdiri atas komputer, software, dan perangkat jaringan lainnya yang bekerja bersama-sama untuk membagi sumber daya, berkomunikasi, dan pengaksesan

informasi. Jaringan komputer telah menjadi bagian dari kehidupan sehari-hari sebagai salah satu media komunikasi dalam bisnis maupun untuk privasi. Untuk menghubungkan beberapa komputer dalam jaringan diperlukan protokol atau aturan dalam berkomunikasi.

Tetapi dibalik kemudahan dalam berkomunikasi di jaringan terdapat lubang kelemahan dari protokol komunikasi tersebut,yaitu kelemahan dari protokol ARP (Address Resolution Protocol) yang melakukan pemetaan terhadap alamat IP (Internet Protocol) dengan alamat MAC (Media Access Control) dari host yang berkomunikasi. Hal tersebut dapat dimanfaatkan oleh para cracker untuk tujuan tidak baik, yaitu spoofing (penyamaran) alamat sebuah komputer dalam jaringan. Teknik penyamaran yang dibahas kali ini dengan cara penyamaran informasi *Hardware address (Ethernet address)* dari sebuah host dijaringan lokal (LAN/Local Area Network).

Seorang *cracker* setelah melakukan *ARP Spoofing* biasanya dilanjutkan dengan serangan-serangan yang bisa melakukan interupsi terhadap dua komunikasi yang sedang berjalan. Jenis-jenis serangan ini antara lain *Man In the Middle*, *sniffing*, *TCP hijacking* atau *session hijacking*.

1.2 Rumusan Masalah

Berdasarkan dari pemaparan yang ada di latar belakang, maka dapat dirumuskan masalah-masalah yang ditampilkan dalam proyek akhir ini, yaitu

1. Bagaimana mencegah atau menangkal penyerangan ARP Spoofing yang terjadi pada sebuah jaringan?
2. Teknologi apa yang digunakan dalam melakukan pencegahan penyerangan ARP Spoofing?

1.3 Tujuan

Tujuan dari proyek akhir ini adalah mengetahui pencegahan atau penangkalan yang dapat dilakukan terhadap serangan ARP Spoofing dan penggunaan teknologi yang mendukung dalam pencegahan atau penangkalan serangan tersebut.

1.4 Ruang Lingkup

Pengimplementasian dan pencegahan yang dilakukan hanya berada diarea yang menggunakan jaringan lokal (LAN/Local Area Network), yaitu Politeknik Telkom.

1.5 Batasan Masalah

1. Spoofing (penyamaran) dilakukan pada jaringan lokal *(LAN/Local Area Network)*.
2. Pembelokan data dilakukan diantara dua buah komputer yang saling berkomunikasi.
3. Tidak membahas algoritma maupun skrip- skrip dari penyerangan dan pertahanan yang terjadi.
4. Tidak adanya jaringan internet.
5. Implementasi hanya terdapat di layer 2 data link (VLAN) dan layer 3 network (ARP).

1.6 Sistematika Penulisan

BAB I Pendahuluan
BAB II Landasan Teori
BAB III Perancangan
BAB IV Implementasi
BAB V Penutup

1.7 Jadwal Kegiatan

Aktifitas	Mei	Juni	Juli	Agustus	September	Oktober	November	Desember	Januari
Identifikasi Aplikasi									
Perancangan									
implementasi									
Dokumentasi									

2. LANDASAN TEORI

2.1 Pengantar Jaringan Komputer

Perkembangan teknologi informasi saat ini merupakan suatu persoalan yang sangat penting. Kemampuan dalam menyediakan informasi secara cepat dan akurat menjadi sesuatu yang sangat esensial bagi suatu organisasi.

2.2 Mikrotik

MikroTik RouterOS™ merupakan sistem operasi Linux base yang diperuntukkan sebagai network router.

2.3 ARP Spoofing

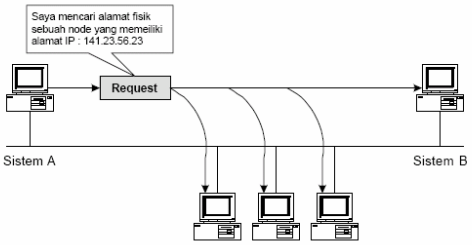
ARP Spoofing merupakan sebuah teknik yang paling efektif untuk menangkap, mendengarkan, dan membajak koneksi antar komputer dalam jaringan[8].

2.4 Firewall

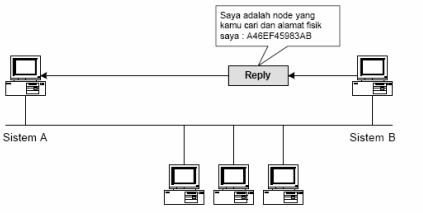
Firewall merupakan suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software atau pun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya.

2.5 ARP (Address Resolution Protocol)

Address Resolution Protocol merupakan proses pencarian alamat *MAC* (*Media Access Control*) komputer dalam sebuah jaringan secara dinamis



Gambar 2.1 ARP Request[6]



Gambar 2.2 ARP Reply[6]

2.6 Sniffing

Sniffing merupakan sebuah usaha untuk menganalisa trafik jaringan dengan mengambil informasi yang berjalan pada sebuah jaringan.

2.7 VLAN

VLAN merupakan suatu model jaringan yang tidak terbatas pada lokasi fisik seperti LAN.

2.8 Bandwidth Management

Bandwidth adalah besaran yang menunjukkan seberapa banyak data yang

dapat dilewatkan dalam koneksi melalui sebuah *network*.

2.9 Aplikasi

Aplikasi yang digunakan pada proyek akhir ini adalah Netcut sebagai aplikasi sang penyerang:

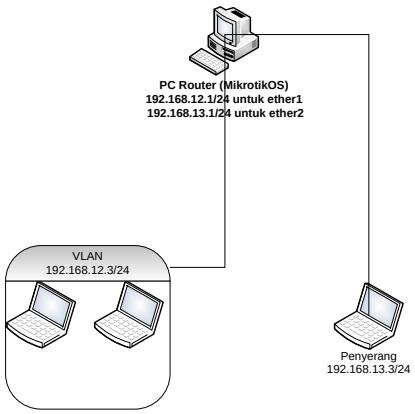
1. **Netcut** : merupakan suatu tool untuk memblok suatu PC untuk mengakses default gateway-nya. default gateway yang dimaksud.

3. PERANCANGAN SISTEM

Pada bab ini akan dijelaskan tentang perancangan pembuatan program untuk melakukan *ARP Spoofing* pada sebuah jaringan lokal (*Local Area Network / LAN*).

3.1 Desain dan Topologi Jaringan

Berikut ini adalah gambar dari desain jaringan yang akan digunakan pada proyek akhir ini untuk menganalisa sebuah serangan *ARP Spoofing* dalam sebuah *Local Area Network* (*LAN*).

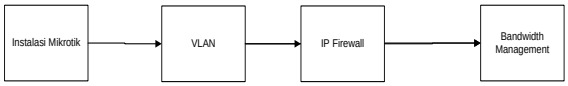


Gambar 1 Simulasi Jaringan

3.2 Desain Aturan Kerja Bandwidth Management

Dalam topologi tersebut, diterapkan *bandwidth management* dengan setiap user mendapatkan *bandwidth* sebesar 512 kbps untuk download dan 128 kbps untuk upload.

3.3 Blok Diagram Pembangunan Sistem



Gambar 2 Pembangunan Sistem

Keterangan :

1. Sebelum pembuatan proyek akhir ini, hal pertama yang dilakukan adalah melakukan instalasi mikrotik dan konfigurasi terhadap alamat IP dari mikrotik,
2. Konfigurasi VLAN terhadap *host* dari luar,
3. Konfigurasi IP firewall pada VLAN untuk otorisasi, agar VLAN dapat mengakses keluar tetapi tidak dapat diakses dari luar VLAN.
4. Melakukan *Bandwidth Management* terhadap jaringan VLAN yang telah terbentuk.

3.4 Tempat Pengujian

Pengujian implementasi penyamaran MAC address pada Proyek Akhir ini dilakukan pada sebuah simulasi sistem jaringan lokal Politeknik Telkom.

3.5 Perangkat Keras

Perangkat keras yang digunakan adalah

1. Laptop
2. PC
    a) Core i3
    b) NIC
    c) RAM 4 Gb
    d) VGA AMD Radeon 5670
3. LAN (RJ 45 Cross dan Straight)

3.6 Perangkat Lunak

Perangkat lunak yang digunakan adalah

1. Mikrotik RouterOS
2. Netcut 2.0
3. Windows 7
4. Vmware 7.0.0 build-203739

3.7 Skenario Penyerangan

Skenario yang terjadi pada sistem jaringan lokal Politeknik Telkom ini adalah

Sebelum pemakaian VLAN dan Bandwidth Management

- User korban melakukan pertukaran data (masuk dalam jaringan lokal).
- User penyerang melakukan scan MAC Address.
- Sesudah melakukan scanning, penyerang memilih IP address/ MAC address yang ingin diputuskan koneksinya.

Sesudah pemakaian VLAN dan Bandwidth Management

- User korban melakukan pertukaran data (masuk dalam jaringan lokal).
- User penyerang melakukan scan MAC Address.
- Sesudah melakukan scanning, penyerang memilih IP address/ MAC address yang ingin diputuskan koneksinya.

4. IMPLEMENTASI

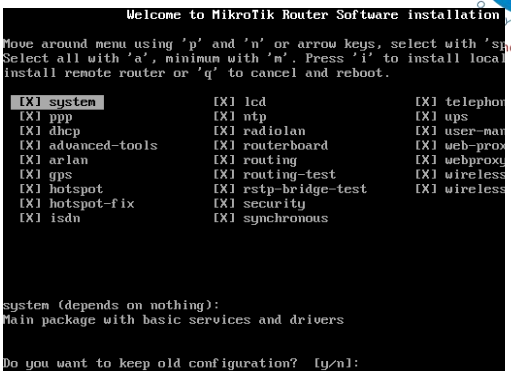
4.1 KONFIGURASI

Berikut merupakan langkah-langkah dalam melakukan konfigurasi dan instalasi yang dilakukan dalam menyelesaikan proyek akhir ini.

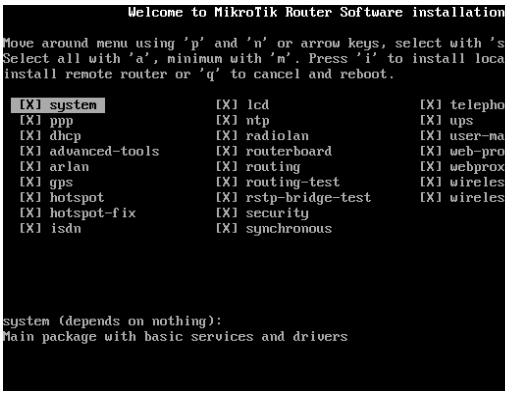
4.1.1Instalasi Mikrotik

Langkah-langkah yang dilakukan dalam proses instalasi *mikrotik* adalah sebagai berikut:

a. Setting *hardware* yang diperlukan oleh mikrotik itu sendiri
b. Lalu untuk pengaturan *Network* Adapter menggunakan koneksi NAT.
c. Jalankan mikrotiknya, dalam interface yang akan muncul pilih “a” untuk menginstal seluruh paket yang tersedia dan “i” untuk menginstalnya.



Gambar 3 Intalasi Mikrotik 1



Gambar 4 Instalasi Mikrotik 2

Keterangan beberapa yang penting diantaranya:

- System : Paket wajib *install* (inti sistem mikrotik/paket dasar), berisi kernel Mikrotik.
- PPP : Point to Point Protocol
- Dhcp : Paket yang dibutuhkan apabila ingin membuat dhcp-server
- Advanced tool : Tools tambahan untuk admnistrasi jaringan seperti ipscan, *bandwidth* test,Scanning, Nslookup dan lain lain.
- Arlan : Paket untuk konfigurasi chipset wireless aironet arlan .
- Gps : Paket untuk support GPS Device.
- Hotspot : Paket untuk membuat hotspot gateway, seperti authentication , traffic quota dan SSL HotSpot Gateway with RADIUS authentication and accounting;
- Hotspot –fix: Tambahan paket hotspot.
- Security : Berisi fasilitas yang mengutamakan keamanan jaringan, seperti remote mesin dengan SSH, remote via MAC address.
- Web-proxy : Untuk menjalankan service Web proxy yang akan menyimpan cache agar trafik ke Internet bisa di reduksi sehingga sensasi browsing lebih cepat
- ISDN : Paket untuk isdn server dan isdn client membutuhkan paket PPP.
- Lcd : Paket untuk customize port lcd dan lain lain.

[x] Kita pilih service apa saja yang ingin kita *install*.

[x] Tekan:

'a' = semua service akan terpilih.

'n' = bila kita meng-*install* baru.

'y' = bila kita hanya ingin menambah service baru (konfigurasi sebelumnya tidak akan hilang)

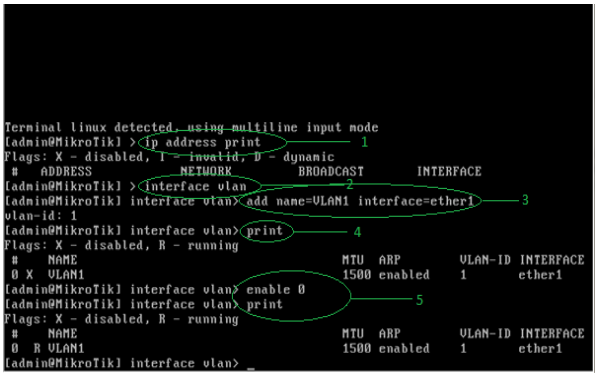
[x] Lalu ketik " i " untuk memulai instalasi, maka proses berlanjut "proses format dan pengkopian *file-file* yang dibutuhkan akan berjalan otomatis"

d. Setelah selesai instalasi, akan reboot secara otomatis dengan menekan Enter, lalu masuk kembali ke tampilan mikrotik.

Gambar 5 Sesudah Instalasi

4.1.2 Konfigurasi VLAN

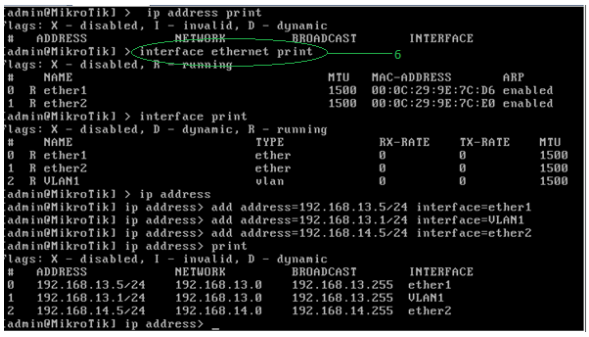
Berikut konfigurasi VLAN pada mikrotik:



Gambar 6 Konfigurasi VLAN 1

Keterangan :

- Ketik “ip address print” untuk dapat melihat IP address pada mikrotik,
- Kemudian masuk ke “interface vlan”,
- Masukkan nama interface VLAN yang diinginkan beserta id-nya,
- Pada *root* “interface vlan” ketik “print” untuk melihat *interface* yang telah dibuat,
- Kemudian ketik “enable 0”untuk mengaktifkan VLAN yang telah dibuat dan ketik kembali “print” untuk melihatnya.



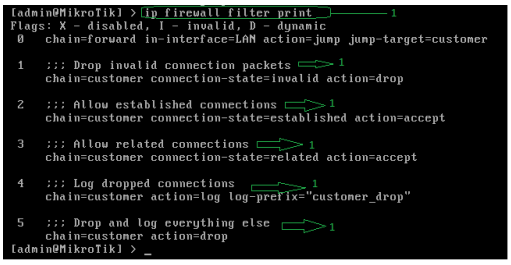
Gambar 7 Konfigurasi VLAN 2

Keterangan :

6. Ketik “interface Ethernet print” untuk melihat *interface* dari Ethernet yang telah ada,

4.1.3 Konfigurasi IP Firewall

Berikut konfigurasi IP *firewall* pada mikrotik :



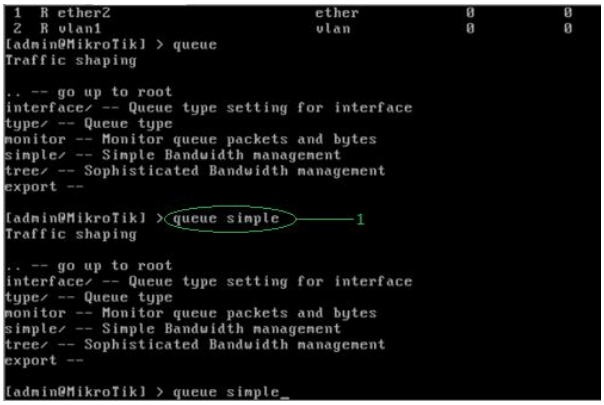
Gambar 10 Konfigurasi IP Firewall

Keterangan :

1. Untuk melakukan otorisasi pada VLAN, dilakukan salah satu fitur dari mikrotik yaitu filtering, dimana bagian dari filtering adalah IP *firewall*.

4.1.4 Konfigurasi *Bandwidth* Management

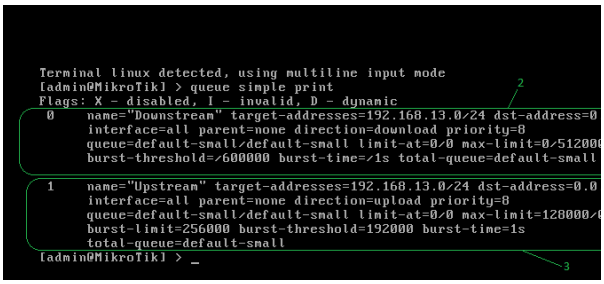
Berikut Konfigurasi *Bandwidth* Management pada mikrotik:



Gambar 11 Konfigurasi Bandwidth Management 1

Keterangan :

1. Ketik “queue simple” untuk melakukan pembatasan bandwidth.



Gambar 8 Konfigurasi Bandwidth Management 2

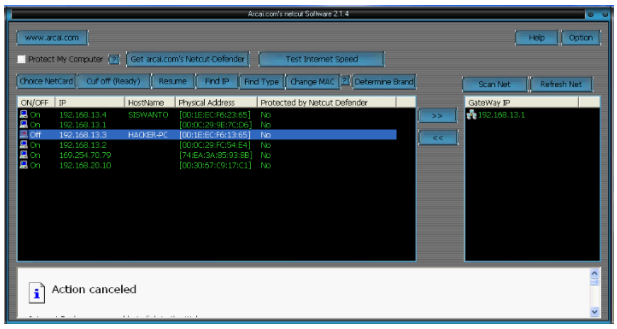
Keterangan :

2. Konfigurasi dari *bandwidth management* untuk aliran data *download* untuk jaringan 192.168.13.0/24,
3. Konfigurasi dari *bandwidth management* untuk aliran data *upload* untuk jaringan 192.168.13.0/24.

4.2 Implementasi Penyerangan

Pada tahap ini, pengujian dilakukan 2 skenario, yaitu tanpa VLAN dan *Bandwidth Management* dengan menggunakan VLAN dan *Bandwidth Management*. Pada setiap skenario yang dilakukan bertujuan untuk memperoleh perbedaan hasil atau dampak penyerangan dari ARP *Spoofing* terhadap pemakaian VLAN dan *Bandwidth Management.*

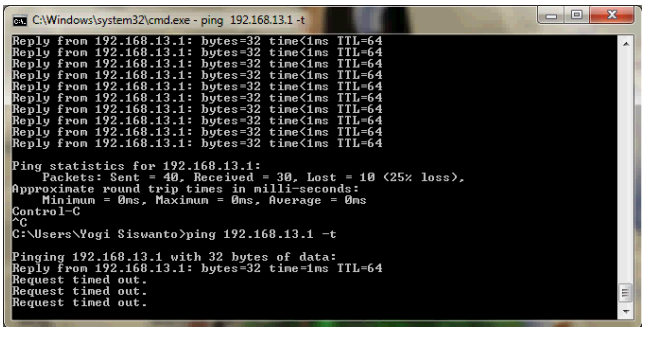
4.2.1 Tanpa VLAN dan Bandwidth Management



Gambar 13 Aksi Netcut 1

Keterangan :

1. Komputer antar *host* dapat melakukan pertukaran data dengan bebas,
2. Tapi ketika diantara host tersebut ada yang mempunyai keinginan jahat dengan menguasai semua jaringan, maka *host* tersebut melakukan ARP *spoofing* dengan memakai aplikasi netcut.

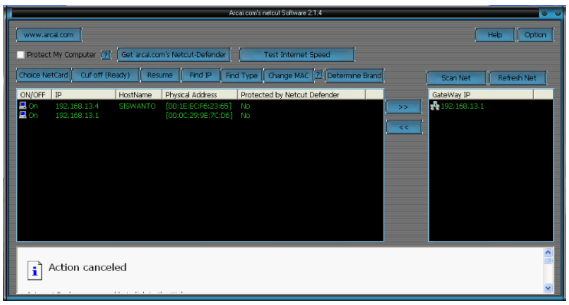


Gambar 14 Dampak Netcut

Keterangan :

1. Setelah pemakain netcut, tampak diatas komputer korban mengalami masalah pada jaringannya, sehingga pengguna dari *host* tersebut tak dapat melakukan koneksi terhadap system jaringan.

4.2.2 Dengan VLAN dan Bandwidth Management



Gambar 15 Aksi Netcut 2

Keterangan :

1. Komputer antar *host* bebas melakukan pertukaran data dalam sistem jaringan,
2. *Host* penyerang ingin melakukan ARP *spoofing*, tapi penyerang tak dapat menemukan alamat IP atau alamat MAC korban ketika menggunakan netcut. Hal itu dikarenakan adanya pembagian(segmentasi) jaringan secara *logic* pada mikrotik berdasarkan VLAN ID, sehingga paket data ARP(alamat palsu) yang dikirimkan penyerangan tak dapat memasuki jaringan VLAN yang memiliki ID yang berbeda karena paket hanya akan diteruskan ke *port* yang memiliki VLAN ID yang sama.

5. PENUTUP

5.1 KESIMPULAN

Kesimpulan yang dapat diambil dari implementasi proyek akhir ini adalah:

1. ARP *spoofing* dapat dicegah dengan pembagian(segmentasi) jaringan secara logic, karena VLAN hanya akan mengirimkan paket data melalui *port* yang memiliki VLAN- ID yang sama sehingga terjadi segmentasi secara *logic*.
2. Metode yang dapat digunakan dalam melakukan pencegahan atau penangkalan serangan ARP *spoofing* adalah VLAN dan Bandwidth Management,
3. Fungsionalitas Bandwidth Management di kanal(*path)* membatasi jumlah paket data, sehingga bila ada penyerang yang ingin memutuskan koneksi untuk mendapatkan *bandwidth* yang besar *bandwidth management* tetap membatasi penggunaan *bandwidth* di setiap kanal.

5.2 SARAN

Saran yang dapat diberi dari implementasi proyek akhir ini adalah:

1. Sebaiknya dalam pemberian VLAN pada Mikrotik harus diikuti dengan fitur lain dari Mikrotik yang bisa mendukung keamanan VLAN itu sendiri, seperti pengaturan otorisasi setiap *host* dengan menggunakan *firewall*.

DAFTAR PUSTAKA

[1] Ahmad Muammar. W. K, "*Firewall"*

[2] Budi Raharjo, "*Keamanan Sistem Informasi Berbasis Internet*", PT Insan Indonesia & PT INDOCISC, Jakarta, 2002

[3] Galia Izenberg, Ohad Barzily, Sharon Vitek, Yaniv Oshrat, *"About ARP"*, Tel Aviv University, 2001

[4] Laurent Licour, Vincent Royer, *"The IP Smart Spoofing"*

[5] Leila Fatmasari Rahman, Rui Zhou, *"IP Address Spoofing"* Seminar Internet-working, Albert-Ludwigs-Universität Freiburg, Institute for Computer Science

[6] Prasimax Technology Development Center, *"Protokol TCP/IP Bagian I"*, Prasimax Technology Development Center, Jakarta, 2002

[7] Sean Whalen, *"An Introduction to ARP Spoofing"*

[8] Silky Manwani, *"ARP Cache Poisoning"*, The Faculty of the Department of Computer Science San Jose State University, San Jose, 2003

[9] echo community, *"Network Security 101: Teori dan Prinsip"* http://echo.or.id [29 Juni 2011]

[10] http://ezine.echo.or.id/ezine7/ez-r07-y3dips-virtual_lan.txt [31 Juli 2011]